IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

TERA WILLIAMS, Individually and on behalf of all similarly situated persons and on behalf of the general public **Plaintiff,** v. **T-MOBILE USA, INC.** CSC-Lawyers Incorporating Service Company 221 Bolivar St. Jefferson City, MO 65101 **Defendant**	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff, Tera Williams, individually and on behalf of all others similarly situated, and on behalf of the general public, upon personal knowledge of facts pertaining to her and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant, T-Mobile USA, Inc. ("T-Mobile"), and alleges as follows:

INTRODUCTION

1. Part of the bargain of purchasing a phone and/or services from T-Mobile includes turning over valuable personally identifiable information ("PII"),[1] including

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII is also generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, or financial account

names, address, Social Security numbers, birth dates, and driver's license information. If left unprotected, identity thieves can gain access to and use this highly sensitive information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in a myriad of schemes, all of which can cause grievous financial harm, negatively affect the victim's credit scores for years, and cause victims to spend countless hours mitigating damage.

2. Every year millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to make the necessary investments to implement important and adequate security measures to protect their customers' and employees' data.

3. T-Mobile, a subsidiary of Deutsche Telekom AG, is one of the world's largest mobile telecommunications companies. T-Mobile is among those companies that have failed to meet their obligation to protect sensitive PII entrusted to them by their current and former customers.

4. As reported by T-Mobile, hackers found their way into T-Mobile's systems, stealing both former and current customer names, birth dates, Social Security numbers and driver's license information of T-Mobile (the "Data Breach").

5. The Data Breach is the fourth breach of T-Mobile's systems since early 2020, and the third in less than a year.[2]

---

number).

[2] *See* https://www.tomsguide.com/news/possible-t-mobile-data-breach (last accessed

6. The cybercriminals responsible for this latest attack began offering Plaintiff's and Class Members' stolen PII for sale the weekend of August 14-15, 2021, according to security researcher Brian Krebs, who predicted that "it would all wind up online soon."[3]

7. Defendant T-Mobile required its customers to provide it with their sensitive PII and failed to protect it. Defendant had an obligation to secure its customers' PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiff and Class Members and T-Mobile.

8. As a result of T-Mobile's failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiff and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here and the fact that the compromised PII is already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiff and the Class, as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.[4]

August 19, 2021).

[3] *See* https://www.latimes.com/business/technology/story/2021-08-18/how-to-protect-yourself-in-t-mobile-hack (last accessed August 19, 2021).

[4] *See, e.g., Resnick v. AvMed, Inc*., 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that the misuse of Plaintiff's sensitive information to open a bank account was sufficient to confer standing even where she did not allege any "unreimbursed losses"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact for data breach case and defining "actual misuse" as a "fraudulent charge"); *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (standing conferred based on alleged fraudulent use of identifying information, without alleged unreimbursed expenses, because

9. Furthermore, Plaintiff and the Class, as also set forth below, will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

THE PARTIES

10. Defendant T-Mobile, a publicly traded company and subsidiary of Deutsche Telekom, is headquartered in Bellevue, Washington, is one of the mobile telecommunication industries' most recognizable brands in the world.

11. T-Mobile is the second-largest wireless carrier in the United States, with almost 105 million customers as of the end of Q2 2021. Of those 105 million customers, roughly 48 million were affected by the Data Breach.[5]

12. Plaintiff Williams is a resident of Kansas City, Missouri and has been a customer of T-Mobile for two (2) years.

13. Plaintiff provided her PII to T-Mobile at T-Mobile's request. Plaintiff reasonably believed T-Mobile would keep her PII secure. Had T-Mobile disclosed to

"the Supreme Court long ago made clear that 'in interpreting injury in fact ... standing [is] not confined to those who [can] show economic harm.'"); *In re Equifax, Inc. Customer Data Security Breach Litigation*, No. 20-10249, 2021 WL 2250845, at *6 (11th Cir. June 3, 2021) (holding that the Plaintiffs plausibly alleged injury in fact and established standing "given the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data…"); *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021) (recognizing that Plaintiffs may establish Article III standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017) ("The principal question, then, is whether the Plaintiff have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have.").

[5] *See* https://www.latimes.com/business/technology/story/2021-08-18/how-to-protect-yourself-in-t-mobile-hack (last accessed August 19, 2021).

Plaintiff that their PII would not be kept secure and would be easily accessible to criminal hackers and third parties and later sold on the dark web as a result, they would have demanded T-Mobile take additional precautions relating to their PII.

JURISDICTION AND VENUE

14. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendant because it is registered to conduct business in Missouri and has sufficient minimum contacts with Missouri.

16. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of its business in this District and Defendant has caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

A. T-Mobile collects and stores millions of current and former customers' PII and has failed to provide adequate data security to protect it.

17. T-Mobile, which is headquartered in Washington with locations in Missouri, is the second-largest wireless carrier in the United States and has annual revenues over $40 billion.[6]

18. Currently T-Mobile, a publicly traded company, has millions of current and

[6] *See* https://www.statista.com/statistics/219435/total-revenue-of-t-mobile-usa-by-quarter/ (last accessed August 19, 2021)

former customers, and is also well-recognized brand on the mobile telecommunications global stage. T-Mobile touts on its website that its privacy principles mean "you can trust us to do the right thing with your data."[7]

B. T-Mobile's inadequate data security exposed its current and former customers' sensitive PII.

19. On August 17, 2021, T-Mobile learned that a bad actor gained access to T-Mobile's systems where highly sensitive customer data was being contained unencrypted.

20. Plaintiff received Data Breach notices in the form of text messages from T-Mobile (collectively, the "Notice").

21. The Notice was sent to Plaintiff via text message. T-Mobile also posted a separate notification of the Data Breach on its website, which included the following information:

> **What happened:**
>
> On August 17, 2021, T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information. The latest details about the affected data are available here.
>
> **Information involved:**
>
> Our investigation is ongoing and this information may be updated. The exact personal information accessed varies by individual. We have determined that the types of impacted information include: names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs (which have already been reset to protect you), addresses and phone number(s). We have no indication that personal financial or payment information, credit or debit card information, account numbers, or account passwords were accessed.

[7] *See* https://www.t-mobile.com/privacy-center (last accessed August 19, 2021).

What we're doing:

> We're relentlessly focused on taking care of our customers – that has not changed. We've been working around the clock to address this event and continue protecting you, which includes taking immediate steps to protect all individuals who may be at risk.

22. After receiving the Notice, it is reasonable for recipients, including Plaintiff and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, especially considering it has already been confirmed that Plaintiff's and Class Members' PII has been made available for sale on the dark web.

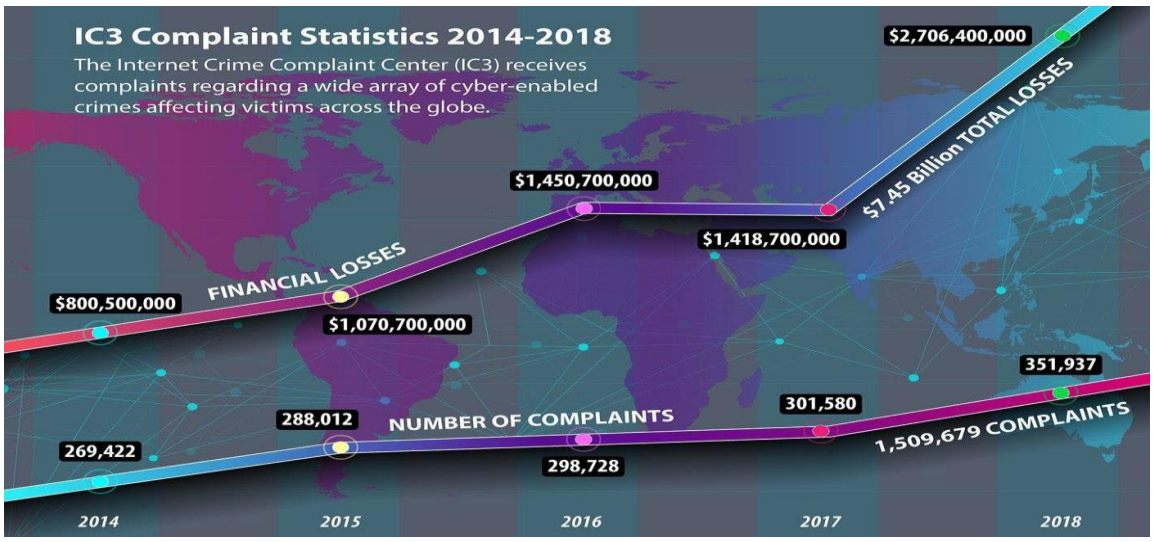
23. As such, it is also reasonable for Plaintiff and Class Members to take steps to mitigate that substantial risk of future harm. In fact, in T-Mobile's online notification to its customers, it warns affected individuals of the potential misuse of their information and that they should, among other things, remain vigilant in reviewing their financial account statements and credit reports for fraudulent or irregular activity, and be alert for phishing emails.[8]

C. The PII exposed by T-Mobile as a result of its inadequate data security is highly valuable on the black market.

24. The information exposed by T-Mobile is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

[8] *See* https://www.t-mobile.com/support/account/additional-steps-to-protect-yourself?icid=MGPO_MTW_U_21DTASECRT_SVFBJIM81C0IT0Q26102 (last accessed August 20, 2021).

25. This exposure, along with the fact that the compromised PII is already being sold on the dark web, is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



26. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[9]

27. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

28. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[10]

29. For example, when the U.S. Department of Justice announced its seizure of

[9] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[10] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed July 28, 2021).

AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[11]

30. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[12]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[13]. Criminals can also purchase access to entire company data breaches from $900 to $4,500[14].

---

[11] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed July 28, 2021).

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 28, 2021).

[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 28, 2021).

31. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems[15].

32. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

33. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

---

[15] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 28, 2021).
[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-

34. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer payment card breach because victims can simply cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

35. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[17]

36. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

37. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

38. Victims of identity theft also often suffer embarrassment, blackmail, or

---

by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 28, 2021).

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 28, 2021).

harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

39. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

40. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[18] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[19]

41. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

D. T-Mobile Failed to Comply with Federal Trade Commission Requirements.

[18] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited July 28, 2021).
[19] *Id.*

42. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[21] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[22]

44. Additionally, the FTC recommends that companies limit access to sensitive

[20] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 28, 2021).
[21] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 28, 2021).
[22] *Id.*

data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[23]

45. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[24]

46. By negligently securing Plaintiff's and Class Members' PII and allowing an unknown third-party cybercriminal to access T-Mobile systems for a fourth time in two years in order to access unencrypted customers' PII, T-Mobile failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data. T-Mobile's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff Williams' Experience

47. Plaintiff Williams became a T-Mobile customer over two (2) years ago.

48. On or around August 19, 2021, Plaintiff Williams received the Notice from T- Mobile informing her of the Data Breach.

---

[23] Federal Trade Commission, *Start With Security*, *supra footnote 17*.

[24] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 28, 2021).

49. As a direct and traceable result of the Data Breach, Plaintiff Williams was forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

50. Plaintiff Williams is careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

51. Plaintiff Williams stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

52. Plaintiff Williams has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Williams entrusted to Defendant to purchase Defendant's products and services. This PII was compromised in, and has been diminished as a result of, the Data Breach.

53. Plaintiff Williams has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces as her PII is being sold on the dark web.

54. Plaintiff Williams has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number and driver's license information, in combination with her full name, which PII is now in the hands of cyber criminals and other unauthorized third parties and being sold on the dark web.

55. Knowing that thieves stole her PII, including her Social Security Number and driver's license number, along with the other PII he was required to provide to T-Mobile, and knowing that her PII is now being sold on the dark web, has caused Plaintiff Williams great anxiety.

56. Additionally, Plaintiff Williams has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She deletes any and all electronic documents containing her PII and destroys any documents that may contain any of her PII, or that may contain any information that could otherwise be used to compromise her PII.

57. Plaintiff Williams has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches, especially considering Defendant's recent history of data breaches.

58. As a direct and traceable result of the Data Breach, Plaintiff Williams will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of her life to protect her exposed PII.

H. Plaintiff and the Class Members suffered damages.

59. The ramifications of Defendant's failure to keep current and former customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[25]

60. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards. Defendant required Plaintiff and Class Members to provide it with their PII, including full names and Social Security numbers. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon products and services being offered by Defendant.

61. Plaintiff and Class Members, therefore, did not receive the benefit of the bargain with Defendant, because providing their PII to Defendant was in exchange for Defendant's agreement to secure it and keep it safe.

62. The Data Breach was a direct and proximate result of T-Mobile's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

63. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former customers' PII, and despite its public statements and representations that T-Mobile would keep their PII safe.

64. Had Defendant remedied the deficiencies in its data security systems and protocols and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

65. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

66. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[26]

67. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts

[26] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed July 28, 2021).

spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant continues to fail to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

68. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft, especially considering Defendant's recent history of data breaches.

69. To date, other than providing a woefully inadequate twenty-four (24) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiff and Class Members.

70. Defendant's failure to adequately protect Plaintiff's and Class Members' PII has resulted in Plaintiff and Class Members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's Notice and website notification indicate, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

71. Defendant's offer of twenty-four (24) months of credit monitoring and identity theft protection services to Plaintiff and Class Members is woefully inadequate. While some harm has already begun, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[27]

CLASS ACTION ALLEGATIONS

72. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

> **Nationwide Class**
>
> All persons residing in the United States who are current or former customers of T-Mobile or any T-Mobile affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff brings this action on behalf of the following proposed Missouri Subclass, defined as follows:

> **Missouri Subclass**

[27] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited July 28, 2021).

> All persons residing in the State of Missouri who are current or former customers of T-Mobile or any T-Mobile affiliate, parent, or subsidiary, and had their PII compromised as a result of the Data Breach.

73. Both the proposed Nationwide Class and the proposed Missouri Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

74. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of T-Mobile; anyone employed by counsel in this action; and any judge to whom this case is assigned, her or her spouse, and members of the judge's staff.

75. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

76. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

f. Whether Defendant engaged in the wrongful conduct alleged herein;

g. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

h. Whether Defendant owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

i. Whether Defendant negligently or recklessly breached legal duties

owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

j. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

k. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PII in violation Section 5 of the FTC Act;

l. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

m. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

77. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

78. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct affected all Class Members in the same manner.

79. **Adequacy of Representation:** Plaintiff is an adequate representative of the

Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

80. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Missouri Subclass)

81. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

82. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care

in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected.

83. Defendant owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former customers.

84. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former customers, especially in light of its recent history of data breaches; Defendant also should have known of the critical importance of adequately securing such information.

85. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard it, that Defendant would not store it longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

86. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Defendant's misconduct included failing to implement the necessary systems, policies, employee training and procedures necessary to prevent the Data Breach.

87. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

88. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

89. Plaintiff's injuries and damages, as described below, are a reasonably certain consequence of T-Mobile's breach of its duties.

90. Because Defendant knew that a breach of its systems would damage millions of current and former T-Mobile customers whose PII was being carelessly maintained, Defendant had a duty to improve its data systems and adequately protect the PII contained therein.

91. Defendant had a special relationship with current and former customers, including with Plaintiff and Class Members, by virtue of their being current or former customers. Plaintiff and Class Members reasonably believed that Defendant would take adequate security precautions to protect their PII. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII.

92. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care

to adequately protect and secure the PII of Plaintiff and Class Members during the time it was within Defendant's possession or control.

93. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third party to access T-Mobile's systems containing the PII at issue, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

94. Defendant's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

95. Neither Plaintiff nor the other Class Members contributed to the Data Breach as described in this Complaint.

96. As a direct and proximate cause of Defendant's actions and inactions, including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiff and Class Members have suffered and/or will suffer concrete injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Missouri Subclass)

97. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

98. Defendant offered products and services to the current or former customers, including Plaintiff and Class Members, in exchange for monetary payment.

99. As a condition of the purchase, Defendant required Plaintiff and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, and other personal information. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon products and services

from Defendant.

100. These exchanges constituted an agreement between the parties: Plaintiff and Class Members would provide their PII in exchange for the products and services provided by Defendant.

101. These agreements were made by Plaintiff or Class Members who were customers of Defendant.

102. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of providing the products and services purchased by Plaintiff and the Class. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members with the bargained-for products and services.

103. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure and/or use.

104. Plaintiff and Class Members accepted Defendant's offer of products and services and fully performed their obligations under the implied contract with Defendant by providing payment and their PII, directly or indirectly, to Defendant, among other obligations.

105. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than the purchase and use of T-Mobile products and services.

106. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' PII.

107. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class Members violated the purpose of the agreement between the parties.

108. Defendant was on notice that its systems and data security protocols were inadequate yet failed to invest in the proper safeguarding of Plaintiff's and Class Members' PII.

109. Instead of spending adequate financial resources to safeguard Plaintiff's and Class Members' PII, which Plaintiff and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class Members.

110. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT III
Breach of Confidence
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Missouri Subclass)

111. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

112. At all times during Plaintiff's and Class Members' interactions with Defendant as its customers, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to

Defendant.

113. Plaintiff's and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

114. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

115. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

116. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

117. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper employee training to secure Plaintiff's and Class Members' PII,

Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

118. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

119. But for Defendant's disclosure of Plaintiff's and Class Members' PII, in violation of the parties' understanding of confidence, Plaintiff's and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

120. This disclosure of Plaintiff's and Class Members' PII constituted a violation of Plaintiff's and Class Members' understanding that Defendant would safeguard and protect the confidential and novel PII that Plaintiff and Class Members were required to disclose to Defendant.

121. The concrete injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew its data security procedures for accepting and securing Plaintiff's and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' PII in jeopardy.

122. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and/or are at a substantial risk of suffering concrete injury that includes but is not limited to: (a) actual identity theft; (b) the

compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

COUNT IV
Invasion of Privacy
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Missouri Subclass)

123. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

124. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

125. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep their PII private and confidential.

126. The unauthorized access, acquisition, appropriation, disclosure,

encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the PII that is the subject of this action, is highly offensive to a reasonable person.

127. This intrusion of privacy was an intrusion into a place or thing belonging to Plaintiff and Class Members that was private and is entitled to remain private. Plaintiff and Class Members disclosed their PII to Defendant as part of their purchases of Defendant's products and services but did so privately with the intention and understanding that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendant's negligent actions and inactions, constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

128. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

129. Defendant invaded Plaintiff's and Class Members' privacy by failing to adequately implement data security measures, despite its obligations to protect current and former customers' highly sensitive PII.

130. Defendant's motives leading to the Data Breach were financially based. In order to save on operating costs, Defendant decided against the implement of adequate data security measures.

131. Defendant's intrusion upon Plaintiff's and Class Members' privacy in order to save money constitutes an egregious breach of social norms.

132. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

133. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiff and Class Members to suffer concrete damages as described herein.

134. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

135. Plaintiff and Class Members have no adequate remedy at law for the injuries they have suffered and are at imminent risk of suffering in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT V
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Missouri Subclass)

136. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

137. In light of their special relationship, Defendant became the guardian of Plaintiff's and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its customers' PII, to act primarily for the benefit of those customers, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' PII and to timely detect and notify them in the event of a data breach.

138. In order to provide Plaintiff and Class Members compensation and employment benefits, or to even consider Plaintiff and Class Members for employment, Defendant required that Plaintiff and Class Members provide their PII.

139. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class Members' PII for the benefit of Plaintiff and Class Members in order to provide Plaintiff and Class Members compensation and employment benefits.

140. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to properly encrypt and otherwise protect Plaintiff's and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiff and Class Members of the Data Breach.

141. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer concrete injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is

used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

142. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Missouri Subclass)

143. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

144. As described above, when Plaintiff and the Class Members provided their

PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiff's and Class Members' PII and to timely detect and notify them in the event of a data breach.

145. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide their PII in exchange for products and services provided by Defendant, as well as an implied covenant by Defendant to protect Plaintiff's PII in its possession.

146. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of certain products and services. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members with the products and services it was offering.

147. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed-upon products and services.

148. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their PII in exchange for T-Mobile's implied agreement to keep it safe and secure.

149. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

150. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII; storing the PII of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendant's data security systems failed to meet applicable legal and industry standards.

151. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

152. Likewise, all conditions required for Defendant's performance were met.

153. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

154. Plaintiff and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

155. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

156. Plaintiff and Class Members are entitled to damages, including

compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT VII
Declaratory and Injunctive Relief
(On behalf of Plaintiff and Nationwide Class or, alternatively, the Missouri Subclass)

157. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

158. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

159. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

160. Defendant owes a duty of care to Plaintiff and Class Members requiring it to adequately secure their PII.

161. Defendant still possesses Plaintiff's and Class Members' PII.

162. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

163. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to

cyberattack.

164. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

165. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

166. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

COUNT VIII
VIOLATIONS OF MISSOURI MERCHANDISING PRACTICES ACT ("MMPA")
MO. REV. STAT. § 407.010 ET SEQ.
(On Behalf of the Missouri Subclass)

167. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

168. RSMo. § 407.020 prohibits the use of any "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce…"

169. An "unfair practice" is defined by Missouri law as any practice which:

(A) Either-

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decision; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers. *See* 15 CSR 60-8.020.

170. An "unfair practice" is also defined as "an unfair practice for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in solicitation, negotiation and performance, or in any manner *fail to act in good faith*" (emphasis added); *see* 15 CSR 60-8.040.

171. Plaintiff and Defendant are "persons" within the meaning of Section 407.010(5).

172. "Merchandise" is defined by the MMPA to include providing "goods" and "services."

173. Efforts to maintain the privacy and confidentiality of customer PII are part of the services associated with a "good."

174. Plaintiff's and the Class Members' goods and services purchased from Defendant were for "personal, family or household purposes" within the meaning of the Missouri Merchandising Practices Missouri Revised Statutes.

175. As set forth herein, Defendant's acts, practices and conduct violate Section 407.010(i) in that, among other things, Defendant has used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of its offered goods and services. Such acts offend the public policy established by Missouri statute and constitute an "unfair practice" as that term is used in Section 407.020(1).

176. Defendant's unfair, unlawful and deceptive acts, practices and conduct include the following: (i) representing to its customers that it would not disclose their sensitive PII to an unauthorized third party or parties; (ii) failing to implement proper security measures such as securing the records in a safe place; and (3) failing to adequately train its personnel.

177. Defendant's conduct also violates the enabling regulations for the MMPA because it (i) offends public policy; (ii) is unethical, oppressive and unscrupulous; (iii) causes substantial injury to consumers; (iv) is not in good faith; (v) is unconscionable; and (vi) is unlawful. *See* Mo. Code Regs. Ann. tit. 15, Section 60-8.

178. As a direct and proximate cause of Defendant's unfair and deceptive acts, Plaintiff and Class Members have suffered damages in that they (i) paid more for T-Mobile

products and services than they otherwise would have, and (ii) paid for privacy protections that they did not receive. In this respect, Plaintiff and Class Members have not received the benefit of the bargain and have suffered an ascertainable loss.

179. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach, the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud.

180. Plaintiff, on behalf of herself and the Class, as well as on behalf of the general public, seeks actual damages for all monies paid to Defendant in violation of the MMPA. In addition, Plaintiff seeks attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of herself and all others similarly situated, and on behalf of the general public, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiff as Class Representative and the undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting T-Mobile from engaging in the wrongful and unlawful acts described herein;

ii. requiring T-Mobile to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring T-Mobile to delete, destroy, and purge the PII of Plaintiff and Class Members unless T-Mobile can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring T-Mobile to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members' PII;

v. prohibiting T-Mobile from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

vi. requiring T-Mobile to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on T-Mobile's systems on a periodic basis, and ordering T-Mobile to promptly correct any problems or issues detected by such

third-party security auditors;

vii. requiring T-Mobile to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring T-Mobile to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring T-Mobile to segment data by, among other things, creating firewalls and access controls so that if one area of T-Mobile's network is compromised, hackers cannot gain access to other portions of T-Mobile's systems;

x. requiring T-Mobile to conduct regular database scanning and securing checks;

xi. requiring T-Mobile to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring T-Mobile to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring T-Mobile to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in

the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with T-Mobile's policies, programs, and systems for protecting PII;

xiv. requiring T-Mobile to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor T-Mobile's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring T-Mobile to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring T-Mobile to implement logging and monitoring programs sufficient to track traffic to and from T-Mobile's servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate T-Mobile's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xx. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxi. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiff and Class Members damages;

f. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Class, as well as on behalf of the general public, hereby demands a trial by jury as to all matters so triable.

Date:

Respectfully submitted,

Maureen M. Brady MO #57800
Lucy McShane MO #57957
McSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108

Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com
ATTORNEYS FOR PLAINTIFFS AND THE CLASS